Federal Risk and Authorization Management Program (FedRAMP)

Four ways to be listed in the FedRAMP repository

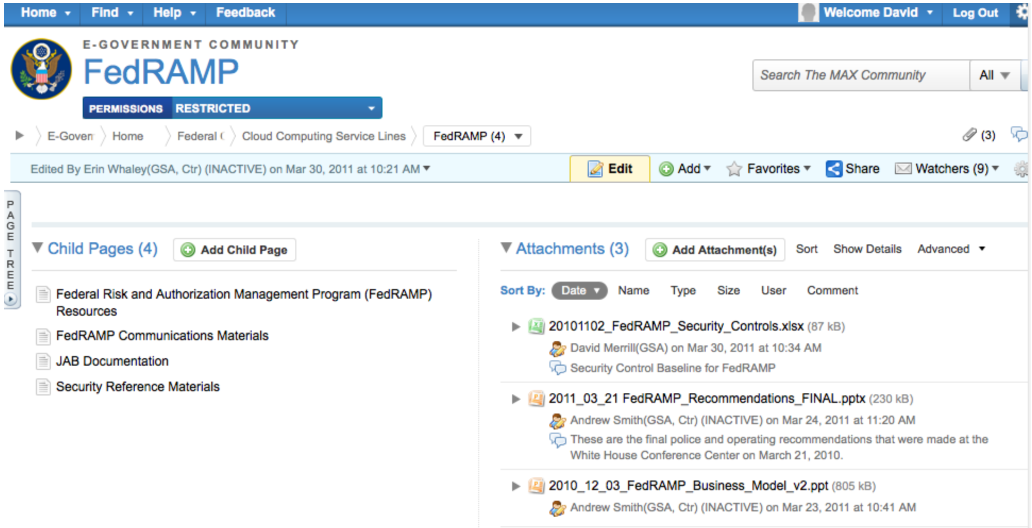
October 25, 2012

Today's Webinar

FedRAMP is a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services.

- This webinar will explain the four (4) different ways that a Cloud Service Provider can have their service listed in FedRAMP's secure repository

What is the Secure Repository?



Edited By Erin Whaley(GSA, Ctr) (INACTIVE) on Mar 30, 2011 at 10:21 AM

- Federal Risk and Authorization Management Program (FedRAMP) Resources
- FedRAMP Communications Materials
- JAB Documentation
- Security Reference Materials

20101102_FedRAMP_Security_Controls.xlsx (87 kB)
David Merrill(GSA) on Mar 30, 2011 at 10:34 AM
Security Control Baseline for FedRAMP

2011_03_21 FedRAMP_Recommendations_FINAL.pptx (230 kB)
Andrew Smith(GSA, Ctr) (INACTIVE) on Mar 24, 2011 at 11:20 AM
These are the final police and operating recommendations that were made at the White House Conference Center on March 21, 2010.

2010_12_03_FedRAMP_Business_Model_v2.ppt (805 kB)
Andrew Smith(GSA, Ctr) (INACTIVE) on Mar 23, 2011 at 10:41 AM

- Enables leveraging of security authorization packages
- Online database of security authorization packages
- Government built, owned, hosted
- Each vendor has a unique enclave within the FedRAMP repository
- Security information is kept current by agencies and CSPs

FedRAMP maintains a repository of standardized security assessment packages Federal Agencies can leverage to make their own risk-based decisions to grant an Authority to Operate for a cloud solution.

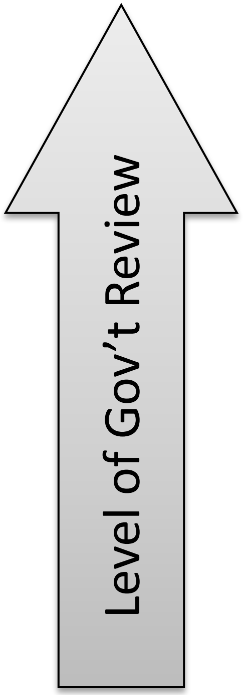
The repository is key to the “do once, use many times” approach.

Key Benefits of Listing in the Repository

- It is the authoritative site for the most current version of CSP’s security packages and provides access to all authorized agency security staff:
  - Conveys a level of trust – documentation is the product of FedRAMP review process and independent testing
- One stop shop
  - One site for agencies to review latest version of documentation
  - One site for CSPs to manage and update documentation
- May reduce the time for deployment of a cloud service within an agency – FedRAMP documentation is the baseline for all agency ATOs

Leverage ATO: FedRAMP Repository

Authorization Level	FedRAMP 3PAO	ATO Status
JAB Provisional Authorization	✓	JAB (+Agency)
Agency ATO with FedRAMP 3PAO	✓	Agency
Agency ATO**	✗	Agency
CSP Supplied	✓	n/a



Level of Gov’t Review

*** A&A packages without a FedRAMP 3PAO do not meet the JAB independence requirements and are not eligible for JAB review*

Repository Listing Requirements

- Common Requirements:

1. Security Control Baseline at appropriate impact level

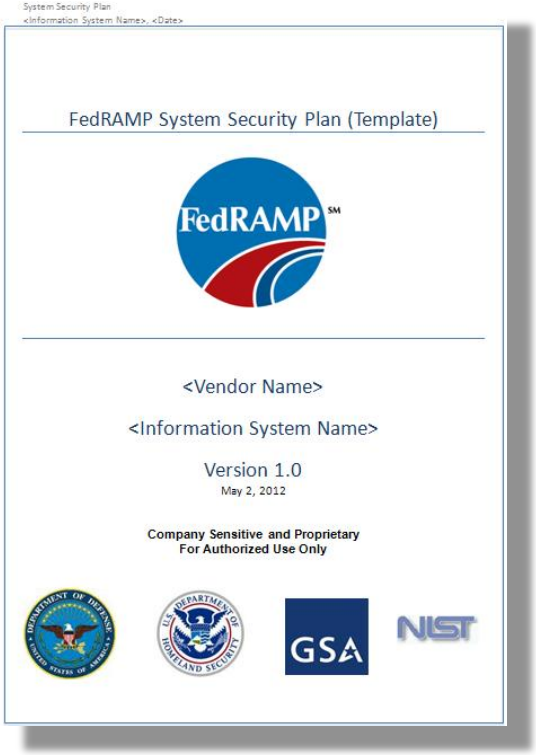
Impact level	NIST Baseline Controls	Additional FedRAMP Controls	Total Controls Agreed to by JAB for FedRAMP
Low	115	1	116
Moderate	252	46	298

2. Assessment by an independent third-party assessor

3. Ensure all security authorization documents are completed and included within the security authorization package.

What documentation must be submitted to be in the repository?

A complete security authorization package includes deliverables in section 10 of the FedRAMP CONOPS



System Security Plan
<Information System Name>, <Date>

FedRAMP System Security Plan (Template)

<Vendor Name>

<Information System Name>

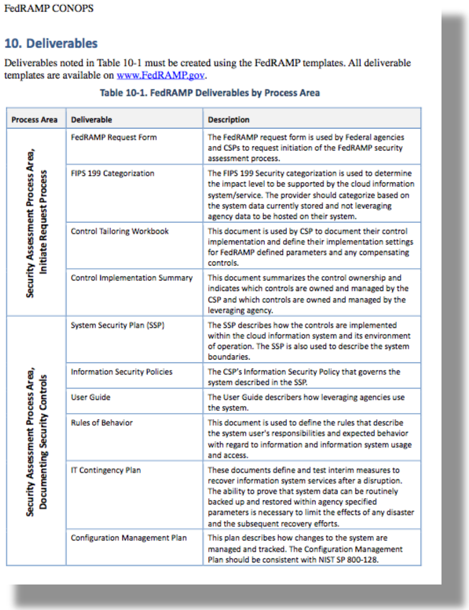
Version 1.0

May 2, 2012

Company Sensitive and Proprietary
For Authorized Use Only

Mandatory Templates:

- System Security Plan
- Security Assessment Plan
- Security Assessment Report



FedRAMP CONOPS

10. Deliverables

Deliverables noted in Table 10-1 must be created using the FedRAMP templates. All deliverable templates are available on www.FedRAMP.gov.

Table 10-1. FedRAMP Deliverables by Process Area

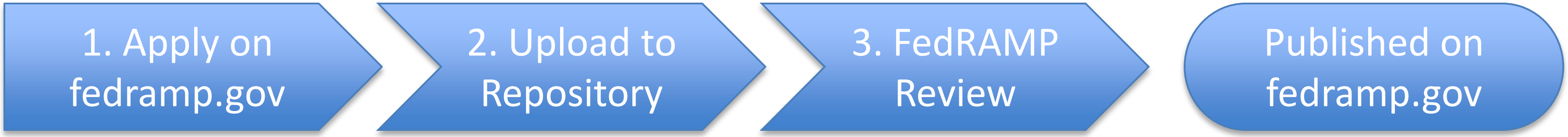
Process Area	Deliverable	Description
Security Assessment Process Area, Initiate Request Process	FedRAMP Request Form	The FedRAMP request form is used by Federal agencies and CSPs to request initiation of the FedRAMP security assessment process.
	FIPS 199 Categorization	The FIPS 199 Security categorization is used to determine the impact level to be supported by the cloud information system/service. The provider should categorize based on the system data currently stored and not leveraging agency data to be hosted on their system.
	Control Tailoring Workbook	This document is used by CSP to document their control implementation and define their implementation settings for FedRAMP defined parameters and any compensating controls.
	Control Implementation Summary	This document summarizes the control ownership and indicates which controls are owned and managed by the CSP and which controls are owned and managed by the leveraging agency.
Security Assessment Process Area, Documenting Security Controls	System Security Plan (SSP)	The SSP describes how the controls are implemented within the cloud information system and its environment of operation. The SSP is also used to describe the system boundaries.
	Information Security Policies	The CSP's Information Security Policy that governs the system described in the SSP.
	User Guide	The User Guide describers how leveraging agencies use the system.
	Rules of Behavior	This document is used to define the rules that describe the system user's responsibilities and expected behavior with regard to information and information system usage and access.
	IT Contingency Plan	These documents define and test interim measures to recover information system services after a disruption. The ability to prove that system data can be routinely backed up and restored within agency specified parameters is necessary to limit the effects of any disaster and the subsequent recovery efforts.
	Configuration Management Plan	This plan describes how changes to the system are managed and tracked. The Configuration Management Plan should be consistent with NIST SP 800-128.

Non-Mandatory Templates

- Control Tailoring Workbook
- Control Implementation Summary
- IT Contingency Plan
- Plan Of Action & Milestones
- Supplier's Declaration of Conformity
- Rules of Behavior
- Incident Response Plan
- Configuration Management Plan

All templates are located on FedRAMP.gov

How does documentation get submitted to the repository?



1. Apply on fedramp.gov

2. Upload to Repository

3. FedRAMP Review

Published on fedramp.gov

- Cloud Service Providers and Federal Agencies apply on FedRAMP.gov
- FedRAMP PMO establishes enclave and grants logins to the secure repository

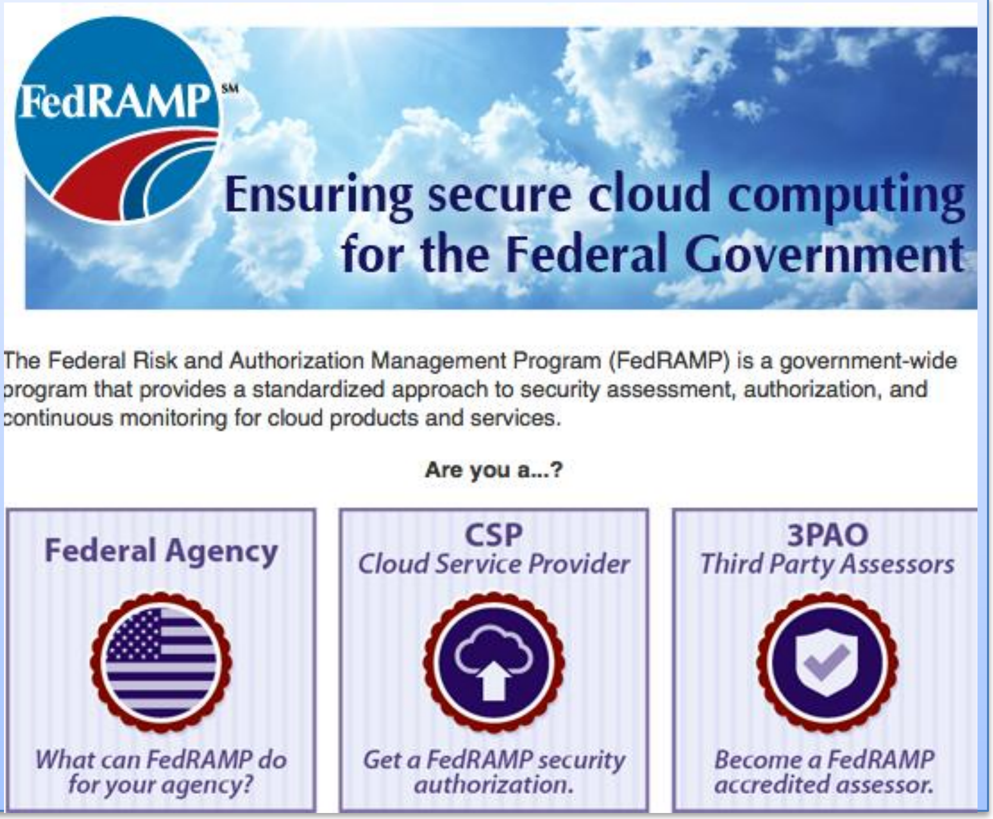
- Cloud Service Provider or Agency uploads completed package
- Agency uploads ATO letter

- FedRAMP PMO check’s package completeness:
- All required documentation?
- All controls in the package?
- No risk reviews

How does an agency use a package in the repository?

Leveraging Agencies search the repository and find:

- Provider
- Date Listed
- Category
- Agency ATO (if applicable)



Ensuring secure cloud computing for the Federal Government

The Federal Risk and Authorization Management Program (FedRAMP) is a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services.

Are you a...?

Federal Agency
What can FedRAMP do for your agency?
CSP
Cloud Service Provider
Get a FedRAMP security authorization.
3PAO
Third Party Assessors
Become a FedRAMP accredited assessor.

- Agencies must implement customer responsibility controls and grant an Agency ATO for the information system residing on the cloud service

Webinar Summary

- 4 ways to be listed within the FedRAMP Repository
- To be listed, CSPs must meet FedRAMP requirements
- Different categories in repository identify different levels of risk authorization
- Use of FedRAMP templates
- Steps for submission for inclusion within the repository
- How agencies will use the repository

Apply on FedRAMP.gov

Question and Answer Session

http://FedRAMP.gov
http://gsa.gov/FedRAMP
Email: info@fedramp.gov

Follow us on twitter @ FederalCloud

Next Webinars:

- November 7: Getting Started with the FedRAMP Security Authorization Process

Upcoming Webinars

- Documenting the FedRAMP Security Controls
- Assessments and completing your security authorization package
- Layering Security Authorization Packages across Infrastructure, Platform, and Software as a service offerings.

For more information, please contact us or visit us at any of the following websites:

http://FedRAMP.gov
http://gsa.gov/FedRAMP
Email: info@fedramp.gov
Follow us on twitter @ FederalCloud